CONFIDENTIAL

# DIGITAL VIDEO DISK COPYRIGHT PROTECTION

## Draft Proposal of the Unified Policy Committee

## Objectives, Timetable, and Methodology

---

**Objectives:**

a) Provide copyright owners with a means to protect copyrighted works distributed to the public on digital video disc media;

b) Allow for expedited introduction to the marketplace of digital video content, and digital video player and recording devices;

c) Avoid imposing unreasonable manufacturing and operational burdens upon computer hardware and software platforms;

d) Allow for reasonable and open access to the technology adopted for implementation of CGMS by new product providers entering the marketplace; and

e) Enable the consuming public to enjoy the fruits of digital video products in an environment of healthy competition between manufacturers of digital video player and recording devices, related interface equipment manufacturers, and content providers.





This document consists of an overview, a summary timeline, and a detailed roadmap. It is intended as a plan for developing a workable copyright protection regime. It is based on the discussions of the DVD technical and policy groups, the principles articulated by CEMA and others, and the documents prepared by BSA members addressing our approach.

**Overview and Basic Approach:**
Casual home copying of motion pictures will be primarily addressed by technical copy protection methods. These copy protection methods will be developed and selected by non-government activities undertaken by single companies or groups of them.

Generally, the use of a given copy protection method will be licensed to users by its originators or by an entity mutually agreed upon. There may be multiple means of protection which compete with or complement each other, all entitled to legal protection as described below. We are currently considering an encryption method, but watermarking technology may be served by this approach as well.

For the encrypt/key exchange method that we expect to be reviewing shortly, an independent non-profit entity (or entities) would perform the functions of:

- Providing **technology licenses** to required interfaces and circuitry,
- Performing **certifications** of devices and systems as compliant with the rules, and
- Granting **authorization codes** to devices and systems which are compliant so that they can access movie content in the approved manner.

To supplement and foster the development of technical copy protection methods, legislation would be drafted. This drafting would address:

- **Anticircumvention**, by specifically outlawing false certifications and authorization codes, as well as a catch-all provision for devices otherwise intended to circumvent.
- **Copyright amendments**, as needed capture the policy compromises struck by HRRC, CEMA, and MPAA.
- **Other** appropriate provisions. See the detailed roadmap.

**A timeline is provided which targets October 1 as the date by which all the most pressing issues are resolved. This is only achievable if we have prompt technical disclosures and continue to stay closely engaged in the solution.**

**Timetable:**

There are three related tracks for activity based on the proposal on the table:
"Private," which relates to individual companies' activities and decisions,
"Entity," which relates to the definition and formation of a standards body, and
"Legis.," which relates to legislative efforts.
The dates are target dates, and are subject to slippage if gating prior events are late.

| Track | Action | Date |
|---|---|---|
| Private | Toshiba/MEI disclosure of technical proposal | ASAP |
| Private | Analyze Toshiba/MEI proposal to determine usability | ASAP |
| Entity | Define Interface Specification for key exchange | Sept 10 |
| Entity | Define "Rules" for entity certification | Sept 10 |
| Entity | Define "Rules" for technology licensing | Sept 10 |
| Legis. | Circulate draft anticircumvention legislation to Policy Commitee | Sept 10 |
| Legis. | Circulate draft other issue legislation to Policy Committee | Sept 10 |
| Legis. | Policy Committee endorsement of legislative proposals | Sept 15 |
| Entity | Establish an interim structure/arrangement for handling certification and authorization codes. | Oct 1 |
| PR | Public announcement of results, transmission to Congress | Oct 1 ~ 30 |
| Entity | Transfer specification "ownership" to a formal standards body, effective on formal adoption. Preferably before year-end. | As soon as stable. |

**Methodology:**

The policy committee will adopt a similar method as has been adopted by the technical committee. Subcommittees will be formed which are committed to delivering workable proposals in the timeframes described. It is proposed that the following subcommittees be established:

Entity Deliverables (see next page)

**Entity Subcommittee-** Would make a detailed proposal on the format of the interim and final managing entities based on the proposals collected here or as later adopted by the Policy Group.
**Certification and Key Management Rules Subcommittee -** Would define the certification methods and rules (including execution rules) to be followed in certification devices as compliant.

Private Activities (second page following) would be carried out by private companies alone or in consultation with others, as well as through the technical groups.

Legislative (third page following)

**Legislative Subcommittee -** would draft and harmonize drafts of legislation that meets the needs articulated below.

**"Entity" Deliverables**

An independent entity would be given responsibility for execution of several tasks. Depending on issues of efficiency, these tasks may be split among multiple entities. The tasks are:

- "Certification" -- evaluation of systems and devices according to fair and nondiscriminatory standards to determine that they are capable of guarding content adequately and are reasonably resistant to tampering. The actual evaluation may be done by the entity itself or by authorized labs (similar to FCC and UL certifications).
- "Authorization Code Distribution" -- providing vendors with the needed codes or secret algorithms that are needed to participate in this protection method. Device authorization codes would only be provided to devices which met certification requirements. To the extent that the "authorization" is in the form of knowing a secret algorithm, a license to the algorithm is included in this activity. This may be handled by a trusted subgroup for security reasons.
- "Interface Licensing" -- The method of delivering key codes and content between devices for purposes of authentication is not part of the protection scheme and would be licensed freely on a royalty-free basis. It is possible and envisioned that protection schemes other than the Toshiba plan may be implemented under the same interface.
- "Technology Licensing" -- DVD Consortium circuitry which implements the interface and algorithms would be licensed by this entity, having received the power to do so under Consortium IP.

Entity Rules

Authorization codes would only be issued to devices which follow the rules. Legislation would guard against circumvention, but the primary defense is the technology itself. The rules for the currently-envisioned scheme are:

- Content may not be decoded unless the rules are all obeyed.
- The device which decodes must be reasonably tamper-resistant, either hardware or software.
- When Content is decoded, no usable copy may be made except (a) for display or (b) in accordance with the rules specified by the copyright owner (encoded in the Content).
- If Content is copy-protected, analog and digital outputs carrying the Content must be copy protected, or degraded to an agreed level, or modified as agreed (*e.g.,* not 60 Hz), or disabled.
- Other rules could be adopted so long as pre-existing content is not unexpectedly exposed.
- HRRC/MPAA legislative compromise may limit exercise of some rules in the transission context.

Entity Life-Cycle

It is desirable to place as many of the above functions as possible with a formal standards body. However, it is not expected that a formal standards body can assume all of the above responsibilities, at least in the timeframe required for rapid execution.

Until a formal body takes over these activities, we would have them handled by a mutually-agreed entity formed for the purpose. In any case, the entity would represent Content owner,

CE, IT, and Recording industry interests, and would be obligated to operate in a nondiscriminatory fashion.

**Private Acitivities**

The entity and legislative proposals for protection of Content are based on the assumption that there will be products, materials and processes worth protecting.

The first apparent instance of a copy protect plan has been described at a high level by Toshiba and Matsushita, who have committed to expedited disclosure of its detailed proposal. The other parties to this process will engage in an evaluation of the Toshiba proposal to determine its suitability for copy protection and adoption for other platforms and implementations. On the assumption that the proposal will meet the needs of other parties, we are proceeding with a plan that takes into account its highest-level features (encryption plus key management).

The DVD consortium has stated that its drive technology will be cross-licensed among its members on a non-discriminatory basis, and that it will license its copy protect circuitry on a royalty-free basis to the industry.

Other industries or developers may develop alternate implementations of the Toshiba method or may, in fact devise entirely separate copy protection and regulation methods. It is expected that the legislation being proposed would protect key aspects of many of these, and that the entity which manages the protection method now under consideration may be appropriate to handle these.

## Legislation

Proposals have been made for legislation. The goals of these laws have been discussed extensively in other documents. Here is an implementation plan:

1. Close on Anticircumvention. Even if nothing else can be accomplished, a reasonable and useful anticircumvention approach will benefit the industry. We believe that a successful anticircumvention proposal will have the following characteristics:

> Prohibition of traffic in, or use of, false encryption keys and authentication codes reasonably expected to circumvent technical copy protection methods, *plus*
> Prohibition of traffic in or use of other devices or methods with primary purpose or effect of circumvention.

2. Close on Mandatory Analog Technology. There is an open debate over whether technology should be mandated for the analog side of the business. Model language should be prepared to crystallize the discussion.

3. Close on Contributory Infringement. Recording and playback devices which do not circumvent should not be subject to charges of contibutory infringement (including 337 actions).

4. Close on Home Recording Rights. So long as it can be drafted so as not to read on software there is no objection to a provision which limits the right to copy-protect motion-picture properties depending on the manner of their transmission.

5. Close on other provisions. Size of penalties and manner of containing liability to reasonable proportions must also be addressed.

**Further Areas:**

Dan Sullivan's memo lays out future technologies and issues to be addressed. I quote:

7.0 Regional codes for playback control could be implemented to support needs of the content owners such as the MPAA, Game authors and other software companies.

> 7.1 DVD-ROM drives should not be "wired " for a region, but be dynamically coded when initially installed or each time the system is turned on.

8.0 Watermarks could be embedded in the active picture area and included in the picture digital data and analog signal regardless of level of MPEG encoding or encryption. These indelible watermarks could form the basis for further anti- piracy auditing and could also be the means by which an Analog signal could be interrogated to determine whether the signal was copy protected and to what extent. Although this proposal does not specifically address the Analog to Digital (AD) issues, this method could greatly facilitate such a process.

> 8.1 Copy Protection methods to inhibit A-D copying should be addressed in future solutions. If watermarks facilitate such future methods, they should be inserted in the content as soon as practicable.
>
> 8.2 Watermarking should not be viewed as on the critical path to launching DVD-Movie players or DVD-ROM drives and applications.

9.0 Future areas to be addressed:

> 9.1 Cable system providers and satellite broadcasting industry groups should be added to the review process prior to the time when final legislation is submitted. Since these two segments will represent means for distributing copy protected digital works, their inputs are important to consider before a congressional debate is conducted.
>
> 9.2 The current DVD basic specifications have left room for a new DVD Audio specification using the DVD technology. In this light, the copy protection method for a combined audio and video content can be applied to the audio only DVD source. The main open item is the concern that current audio CD's could be copied onto a DVD-RAM or right-once media without the degradation caused by analog tape recordings. Additional discussion needs to take place to determine the business model the RIAA wants to perpetuate and how this can be incorporated in the current activity

DRAFT
ANTI-CIRCUMVENTION PROVISION
FOR ENCRYPTED, DIGITAL SOURCE
LINEAR MOTION PICTURES JAB; 8/5/96

CONFIDENTIAL

(a) It shall be unlawful and subject to the actions and remedies prescribed in § ____ to ***interfere with*** a ***qualified self-protection system.***

(b)(1) A ***qualified self-protection system*** means a process or technique that --

(A) by encryption or scrambling, renders a linear motion picture fixed in a copy or included in a transmission, in digital format, unintelligible to consumers until decrypted or descrambled, by application of a particular process or technique anticipated by the copyright owner of the linear motion picture; and

(B) permits control over the making of a copy, in digital format or in analog NTSC format, of an intelligible rendering of a linear motion picture directly or indirectly from a copy or transmission fixed or made in encrypted or scrambled digital format; and

(C) has been adopted by a recognized standards-setting body in the United States consistent with such body's usual rules and procedures [and] [,or] has been widely implemented in the United States by copyright owners of linear motion pictures;

(2) For the purpose of paragraph (c), a ***qualified self-protection system*** includes those aspects (including processes and conditions, whether anticipated by a standard or imposed by a license or similar authorization) of or related to such system that may pertain --

(A) to decryption, de-scrambling, or similar process of rendering a linear motion picture fixed or transmitted in digital format intellgible to consumers;

(B) to control (including the activation and detection of, and response to, pertinent embedded or appended data or other properties) -- by prohibition, inhibition, or limitation -- of the copying of a linear motion picture directly or indirectly from a copy or transmission fixed or made in encrypted or scrambled digital format; or

(C) to the transfer among devices, or the prohibition or conditions of such transfer, of a signal embodying a linear motion picture in any analog or digital format, provided that such signal, if it has been translated or converted, originated with a copy or transmission fixed or made in encrypted or scrambled digital format;

(D) to playback from any copy made directly or indirectly from a copy or transmission fixed or made in encrypted or scrambled digital format, or to any other performance or display of a linear motion picture from an authorized copy or transmission fixed or made in encrypted or scrambled digital format.

(c) To ***interfere with*** a ***qualified self-protection system*** means --

(1) to manufacture or distribute in the United States, or import into the United States, any linear motion picture recording or interface device or freely programmable general-purpose computer, or any component that may be or is connected to or incorporated into any such machine or device, that, upon and after initiating any procedures or processes to encrypt, de-scramble or otherwise render intelligible a linear motion picture in digital format that has been encrypted, scrambled, or similarly treated in accordance with [any] qualified self-protection system [in existence within months before the date of such manufacture, distribution, or importation] does not in its design, configuration, or construction comply with such ***qualified self-protection system***;

(2) to manufacture or distribute in the United States, or import into the United States, a machine or device, or any component that may be or is connected to or

incorporated in any machine or device, the reasonably foreseeable effect of which is to assist or enable another person to avoid, bypass, remove, deactivate, or otherwise defeat or circumvent the application or operation of any aspect of any ***qualified self-protection system*** [in existence within _____ months before the date of such manufacture, distribution, or importation] or any analog protection system described in clause (c)(3); provided that this paragraph does not apply to a linear motion picture recording device or freely programmable general purpose computer that does not violate paragraph (1) of this section.

(3) to manufacture or distribute in the United States, or import into the United States, any recording device that is designed and marketed to allow consumers to record a linear motion picture in analog format unless such device effectively responds to an analog protection system that is [substantially identical to an analog protection system identified in a ***qualified self-protection system*** in connection with analog outputs of digital devices] [identified in § ___ of this chapter].

(4) for the purpose of copying a copyrighted linear motion picture or portion thereof, to engage in any conduct or perform any service the purpose or reasonably foreseeable effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent the application or operation of any ***qualified self-protection system*** or any analog protection system described in paragraph (c)(3); provided: that no liability shall exist under this paragraph by reason of the mere manufacture, distribution, or importation of a machine or device that does not violate paragraph (1) or (2) of this section.

(5) to obtain, disseminate, or use, without proper authorization, or in material breach of the terms of such authorization, any decryption, descrambling, or similar key, algorithm or element pertaining to a ***qualified self-protection system.***

(6) to act in a material breach of any license, agreement, or undertaking pertaining to the permitted use of

technology relevant to implementing a ***qualified self-protection system.***

CONFIDENTIAL